Chief Information Officer's Section
Office of the Governor
State of Utah

July 26, 2002

Virus Detection Policy

Policy Objectives and Scope: For purposes of this policy, a computer virus is an executable program, macro, etc. It is designed to replicate itself to spread onto local and network storage media, email itself to users address books or even to hosts on the local network or the Internet for the purpose of mischief, damage, or attack on other systems (while recognizing that there are benevolent viruses written to repair the damage from, or eradicate malicious code; for purposes of this policy, viruses will be considered primarily malicious). The objective of this policy is to define common terms relating to computer viruses, define a standard level of virus protection methods as well as response and removal procedures.

Defintions:
Virus: executable program fragment that reproduces by attaching itself to another program. It is designed for malicious and, or mischievous purposes and when functioning properly degrades performance on the host computer, the network, consuming system resources or damaging, altering or deleting files on the host. Human interaction triggers virus activity, viruses do not propagate without it.

Worm: An independent program that reproduces by copying itself from one system to another, primarily targeting networks to slow or even shut them down. Unlike viruses, worms do not require human interaction to propagate.

Trojan Horse: An independent program that appears to perform a useful function while hiding unauthorized executable code that performs unauthorized functions while the user is attempting to execute the program according to its advertised function (including usurping the privileges of the user or compromising confidential information.

Infection: When a virus, worm, Trojan Horse, or variant successfully installs on a host and executes according to its design, causing network or host degradation, damage or otherwise interfering with normal operations.

Virus Removal Software: Software designed to detect virulent activity on the host computer or network detect changes in critical configuration, environment, system, or executable files and respond by disabling or removing the perpetrating virus.

All computers should run anti-virus software: Computers having trusted (internal) access to State of Utah network resources must run current anti virus software that complies with State software standards. Anti virus software will be managed by the agency LAN (Local Area Network) administration team under the supervision of administrators knowledgeable in networking, PC's (Personal Computers), email and operating PC Servers. Individual users should not be able to interfere with or disable its function.

Updates: A computer virus specialist, acting in cooperation with ITS an the CIO's office will notify LAN administrators of software updates and provide a deadline for installing updates. Updates will be automatically installed on PCs without users intervention as often as they are available.

~~**Software Installations:** All software installed on PCs, servers, etc., having trusted access to the State of Utah WAN shall be installed by, or under the supervision of LAN administrators~~

~~employed by or contracted to the State for the purpose of LAN administration. The user shall install no other software without express permission extended by the agency LAN administrator manager.~~

Electronic Mail (email): The State email gateways shall be configured to block attachments fitting known virus descriptions, executable programs (.exe, .com), system files (.sys, .dll), batch (.bat) and other files known to spread malicious programs. Users will be trained in recognizing potentially dangerous emails and in responding appropriately to virus warnings.

Response: When a virus is detected, the user should follow help desk procedures, submitting a request for assistance. The LAN administrator will then determine if the anti-virus software has successfully disabled and/or removed the virulent program. If the LAN administrator is unsuccessful in removing the virus, the computer system will be removed from the network and hard drive will be formatted with a new master boot record.

Product Recommendations: Where practicable virus detection software should be used by all agencies. Any virus detection product used must provide continuous virus protection, on demand virus scanning of PC's and servers, file quarantine capability, and automatic virus update functionality. Virus detection/correction software procurement must be coordinated through the Division of Purchasing for optimal pricing.

References:

Interim Date: Pending
Organization Sponsoring the Standard: ITS, State Information Security Committee (SISC)
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: 6/27/02 for comment
Author(s): Rick Gee (ITS)
Related Documents: State Information Security Policy, State Network Access Policy